CLAIMS

1/ A method of modifying the content of the non-volatile memory of a microcircuit card, in particular a contactless card,

in which method the card is temporarily coupled to a terminal while a transaction is being executed, in particular a remote ticketing transaction, the transaction including the terminal applying to the card a plurality of modification commands, each comprising at least one operation of recording in the card memory a respective data item designated by the command, the various data items recorded in this way being mutually interdependent,

the method being characterized in that it comprises the card executing the following steps:

a) on receiving corresponding respective commands from the terminal, it modifies the contents of the card memory by provisionally recording in the card memory each of said interdependent items of information without losing prior values corresponding to said items; and then

b) the modifications are finalized either by all of them being confirmed or by all of them being discarded, such that for subsequent operations, the commands executed in step a) will either all have been taken into account, or else all of them will be without effect.

2/ The method of claim 1, in which:

· in the event of confirmation in step b), a flag confirming proper execution is recorded in the memory of the card; and

· when the card subsequently receives a command requiring at least one of the data items written in step a) or the value corresponding thereto to be read and/or modified, the card begins by examining the state of the flag, and if it has not been recorded, the card ignores or cancels the provisional recordings previously made in

step a) and executes the command on the basis of said prior values corresponding to the data items.

3/ The method of claim 2, in which, when the card examines the state of the flag, and if the flag has been recorded, the card executes operations for copying the provisional writes made in step a).

4/ The method of claim 1 ~~or 2~~, in which the card is suitable for operating in two modes, namely:

· an in-session mode in which recordings are made by executing steps a) and b); and

· an out-of-session mode in which the making of recordings is not confirmed to all of steps a) and b).

5/ The method of ~~any one of claims 1 to 4~~ claim 1, comprising an authentication function combined with the function of finalizing step b), forcing step b) to be discarded in the event of authentication failing.

6/ The method of claim 5, in which said authentication is performed by the card which authenticates the terminal and/or the data interchanged between the terminal and the card, the card checking a cryptographic certificate produced by the terminal and transmitted to the card, and confirming the modifications in step b) only if the certificate is recognized as being correct.

7/ The method of claims 4 ~~and 6~~ taken in combination, in which, when the card receives from the terminal commands for modifying the content of the memory and including verification of a cryptographic certificate, said verification is performed if the command is received out-of-session, and it is not performed if the command is received in-session.

8/ The method of claim 5, in which said authentication is performed by the terminal which authenticates the card and/or the data interchanged between the terminal and the card, the card producing and transmitting a cryptographic certificate in conditional manner to the terminal, if and only if the modifications have been confirmed in step b).

9/ The method of claims 4 ~~and 8~~ taken in combination, in which, when the card receives from the terminal commands for modifying the contents of the memory and including the production of a cryptographic certificate, said production is performed if the command is received out-of-session, and is not performed if the command is received in-session.

10/ The method of claim 1 ~~or 2~~, in which, when the card receives from the terminal in step b) commands for modifying the contents of the memory and including the production of a plurality of cryptographic certificates, these certificates are stored in step b), and then transmitted together to the terminal if, and only if the modifications have been confirmed in step b).

11/ The method of claims 1 ~~and 4~~ taken in combination, in which at least some of the commands that may be executed in step b) include an optional inhibit attribute, and in which, if the card executes such a command in-session in a step b), the modifications performed by said command take effect independently of the result of step b).

12/ The method of claim 1 ~~or 2~~, in which provision is further made, after step b) and in the event of modifications being confirmed, for the following sequence of steps to be performed:

d) the terminal executes an action following confirmation by the card; and

e) in the event of said action being properly performed by the terminal, ratification information is recorded in the card suitable for subsequent accessing by reading.

13/ The method of claim 12, in which the recording command of step e) is an implicit command, any command received by the card after step b) being interpreted as an order for recording ratification information in the card.